COPY

CRIMINAL COMPLAINT

UNDER SEAL

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA V. JARED JAMES ABRAHAMS	Docket No. MAGISTRATE'S CASE NO. SA13-422M

Complaint for violation of Title 18, United States Code, Section 875(d)

NAME OF MAGISTRATE JUDGE	TITLE	LOCATION
HONORABLE ROBERT N. BLOCK	UNITED STATES MAGISTRATE JUDGE	Santa Ana, CA

DATE OF OFFENSE	PLACE OF OFFENSE	Address of ACCUSED (IF KNOWN)
March 21, 2013	Orange and Riverside Counties	

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

On or about March 21, 2013, in Orange County and Riverside County, in the Central District of California, and elsewhere, defendant JARED JAMES ABRAHAMS, knowingly and willfully, and with the intent to extort money and other thing of value, did transmit in interstate and foreign commerce from Providence, Utah to Temecula, California, an email communication to victim C.W., and the email communication contained a true threat to injure the reputation of C.W.

FILED
CLERK, U.S. DISTRICT COURT
SEP 17 2013
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:

See attached affidavit which is incorporated as part of this Complaint.

MATERIAL WITNESSES IN RELATION TO THIS CHARGE: Not Applicable.

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.

SIGNATURE OF COMPLAINANT

/s/

Julie Patton
Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

SIGNATURE OF MAGISTRATE JUDGE*	DATE
ROBERT N. BLOCK	9/17/13

* *See* Rules 3 and 54 of the Federal Rules of Criminal Procedure.

AUSA: VM:ll

VM

A F F I D A V I T

I, Julie Patton, being duly sworn, hereby state as follows:

I.

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 1996. I am currently assigned to the Cyber Crime squad in the Orange County, California, resident office. In that assignment, I specialize in the investigation of computer and high-technology crimes, including computer intrusions, denial of service attacks, identity theft and theft of personal financial data, and other types of malicious computer activity. During my career as an FBI SA, I have participated in numerous investigations, including computer crime investigations. In addition, I have received both formal and informal training from the FBI regarding computer-related investigations and computer technology.

2. The facts set forth in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this affidavit is being submitted for the limited purpose of supporting a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish that probable cause exists that JARED JAMES ABRAHAMS ("ABRAHAMS") violated Title 18, United States Code, Section 875(d).

II.

PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a criminal complaint, charging ABRAHAMS with violating Title 18, United States Code, Section 875(d) (extortion).[1]

III.

BACKGROUND

4. The following definitions relate to the Internet, email, and other computer tools as they apply to the activity discussed in this affidavit[2]:

a. AOL, Inc. ("AOL"): AOL, Inc., also known as "AOL" and "America Online," is a corporation that provides, among other things, email accounts to its users. AOL email accounts end with aim.com or aol.com. I spoke to a representative from AOL who confirmed that their email servers have been located in Virginia since before 2012. Based on my training and experience, including conversations with an AOL representative, I know that when a user receives or sends an email message using AOL email addresses ending in aol.com or aim.com, the message will first go to an AOL email server residing in Virginia.

b. Email: Email, also known as "electronic mail," is a popular means of transmitting messages and/or files in an

---

[1] Title 18, United States Code Section 875(d) states as follows: Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

[2] The definitions provided here are based on my training and experience, as well other sources, including research.

electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

c. Internet: The Internet is a collection of computers, computer networks, and devices that are connected to one another via high-speed data links and telephone lines for the purpose of communication and sharing data and information. Connections between Internet-enabled computers and devices exist across state and international borders; therefore, information sent between two devices connected to the Internet frequently crosses state and international borders even where the two devices are located in the same state.

d. Internet Protocol ("IP") Address: An Internet Protocol or "IP" address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g, 128.195.188.231). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most Internet Service Providers control a range of IP addresses.

e. Internet Service Provider ("ISP"): Many individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers, or "ISPs." ISPs provide their customers with access to the Internet using telephone or telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the

ISP's servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. These records often include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, and other information both in computer data and written record format.

f. Keyloggger: A keylogger is a computer program that records every keystroke made by a computer user. Keyloggers are often used in order to gain fraudulent access to passwords and confidential information. Malware (as described below) uses keyloggers to store in a file (a "keylog file") the keys struck on a keyboard in a covert manner so that the user does not know that his or her keystrokes are being recorded.

g. Malware: Malicious software or "malware" is software that, among other things, allows malicious computer users to gain remote access to victim computers without authorization and collect sensitive information from the computer.

h. No-ip.org: No-ip.org is a website offering dynamic domain name resolution. This service can be used to hide the actual IP address of a hacker or other user. Ordinarily, malware might allow a hacker to connect directly to a victim's computer or through another computer that the hacker controls. With no-ip.org, once installed on a victim's computer, the malware can connect to a no-ip.org account -- as opposed to an IP address easily identifiable as the hacker's to control the malware. This feature also enables the malware to continue to work should the hacker's IP address ever change.

i. Nslookup: Nslookup means "name server lookup." A nslookup is an application used to determine the domain name or IP address for a specific Domain Name System ("DNS") record.

j. Remote Administration Tool ("RAT"): A RAT is a software application that allows a remote operator to control a system as if he has physical access to the system. It is typically undetectable to the user of the computer.

k. Sextortion: Sextortion is a type of extortion and/or blackmail of a victim. The victim is extorted and/or blackmailed with a nude image of the victim. The person committing the sextortion threatens to release the nude image publicly unless the victim, among other things, performs a sexual act. The person committing the sextortion is typically threatening to harm the reputation of the victim by disclosing the nude image.

l. Skype: Skype is a division of Microsoft Corporation that offers an application which allows people to, among other things, video chat on the Internet. A Skype user, with his or her computer, can communicate with another person using text, voice, and video.

m. Slave Computer or "Slave": A slave computer or "slave" is a term used in the computer industry and by computer hackers to refer to a device, including a computer, that another device has control over. For example, hackers that use RATs to remotely control a victim's computer refer to the victim's computer as the hacker's slave computer or "slave."

n. Social Engineering: Social engineering is, among other things, the exploitation of human psychology to gain access to building, systems, or data. Social engineering techniques include pretexting and phishing where victims are duped into disclosing information or performing acts because the

victims believe they are communicating with a legitimate business, authority, or person.

o. Virtual Private Network ("VPN"): A Virtual Private Network is a tool often used to hide the identity of users while online. When an individual uses a VPN, the IP address assigned to the user's online activity will resolve to a location hosted by the VPN business. An individual's identity is protected because the VPN does not keep logs of which users used their ISP at which specific times and dates.

IV.

SUMMARY OF PROBABLE CAUSE

5. During an investigation that began in or around March 2013, I learned that ABRAHAMS compromised victims' computers and obtained nude photographs and/or videos of the victims through remote operation of the victims' web-enabled cameras ("webcams"). After taking the nude photographs and/or videos, ABRAHAMS contacted some victims using two AOL, Inc. ("AOL") email accounts (collectively, "AOL email accounts") he had taken over. One of the AOL email accounts ended in aim.com ("F.L. aim.com") and the other ended in aol.com ("F.L. aol.com"). ABRAHAMS also contacted some victims using an email address ending in outlook.com ("P.S. outlook.com")[3]. When ABRAHAMS contacted the victims by email, the victims learned that ABRAHAMS had remotely used the victims' webcams to take nude photographs and/or videos of the victims without their consent because ABRAHAMS would generally attach some of the nude photographs and/or videos he had.

6. In emails (which ABRAHAMS often sent while using a Utah-based VPN service), ABRAHAMS threatened to publicly disclose on the victims' Internet social media accounts the nude photographs

[3] Outlook.com is a free, web-based email service offered by Microsoft Corporation.

and/or videos unless the victims did one of three things: (1) sent nude photographs, (2) sent a nude video, or (3) logged on to Skype and did what ABRAHAMS told the victim to do for five minutes. In one instance, ABRAHAMS threatened (by disclosing nude photographs of the victim) to transform a victim's "dream of being a model . . . into [the victim being] a pornstar" if the victim did not comply with his demands.

7. On June 4, 2013, federal search warrants were executed by agents and detectives at ABRAHAMS's residence in Temecula, California. During the search, agents seized digital devices of ABRAHAMS, including a computer, a laptop, cell phone, and thumb drives. The digital devices were later found to contain (as described in more detail below): evidence of hacking software and malware used to take over the victims' computers and images and videos of some of the victims.

8. During the execution of search warrants at his residence, ABRAHAMS voluntarily agreed to speak with me and another agent. As described below, ABRAHAMS admitted to infecting people's computers with malware; watching his victims change their clothes; and using photographs against his victims. ABRAHAMS admitted that C.W. was the first person (whose computer he hacked) that ABRAHAMS knew personally. ABRAHAMS admitting to getting a victim, M.M. #1, to go on Skype and take her clothes off at his direction. After the Skype session, ABRAHAMS pretended to delete the original photos he had (of M.M. #1).

V.

PROBABLE CAUSE STATEMENT

Eighteen-Year-Old, C.W., Received Extortion Emails

9. I interviewed an eighteen-year-old woman, C.W., who told me that she learned on March 21, 2013, that her laptop computer had been compromised because she received an alert from Facebook that someone was trying to change her account password. She

subsequently learned that her Twitter, Tumblr, and Yahoo! email passwords had been changed and that someone had changed her Twitter profile picture to a half nude picture. About thirty minutes after the first notification from Facebook, she received an email message from F.L. aim.com (later identified as an email address taken over by ABRAHAMS) at her Yahoo! email account.

a. The email included two attachments that C.W. recognized as nude photographs of herself taken in her current Riverside County residence. The nude photographs appeared to be taken from her laptop's webcam without her knowledge. Based on the background furnishings in some of the other photographs attached to the email, C.W. concluded that those photographs were taken several months earlier, when she lived in Orange County, California.

b. The message read, in part, as follows: *"Here's what's going to happen! Either you do one of the things listed below or I upload these pics and a lot more (I have a LOT more and those are better quality) on all your accounts for everybody to see and your dream of being a model will be transformed into a pornstar. Do one of the following and I will give you back all your accounts and delete the pictures. 1) Send me good quality pics on snapchat 2) Make me a good quality video 3) Go on skype with me and do what I tell you to do for 5 minutes If you don't do those or if you simply ignore this then those pics are going up all over the internet. It's your choice :) Also I'm tracking this email so I'll know when you open it. If you don't respond then your pics are going up."*

c. C.W. told me she has never knowingly taken or allowed anyone to take nude photographs of her.

10. The messages from F.L. aim.com were examined by FBI agents. Each message header showed an originating IP address of 174.127.99.190. According to Centralops.net (an online tool for

searching IP addresses), that IP address resolves to Hosting Services, Inc., Providence, Utah. The agents determined that Hosting Services, Inc. is a VPN service which advertises that it does not keep logs.

11. The email account F.L. aim.com is an email account provided by AOL. I obtained and reviewed records from AOL which showed that F.L. aim.com was accessed 35 times between March 22, 2013, and April 2, 2013. All, except two of these accesses, were made through IP address 174.127.99.190, the same Utah-based VPN which had been originally used by the person sending C.W. threatening emails, who was later identified to be ABRAHAMS.

Message Header Information Showed that ABRAHAMS Used VPNs to Make Tracing Difficult

12. I applied for and obtained a court-authorized pen register and trap and trace device to be placed on the AOL email accounts (F.L. aim.com and F.L. aol.com) which ABRAHAMS used to send emails to C.W.

13. From the data I received and reviewed, I learned the following:

a. Between April 11, 2013, and April 18, 2013, header information from the two AOL email accounts contained the IP address associated with the Utah VPN, 174.127.99.190, as well as a second IP address, 173.254.223.67, which was associated with a VPN server in the Los Angeles area.

b. Between March 28, and May 20, 2013, there were at least sixty emails between the two AOL email accounts and C.W.'s Yahoo! email account.

c. Some of the email headers were notifications from "bananatag," an email productivity application (distributed by a Canada-based company) I had previously seen being used in ABRAHAM's communications with C.W. "bananatag" and "Toutapp"

were both used by ABRAHAMS as a tool to get notifications when his victims read his email messages.

d. There were other bananatag notifications and header information to and from other email recipients, which appeared to be additional victims of ABRAHAMS. The victims included E.L., M.M. #1, and G.B. This was later confirmed when I observed an email received by C.W. which contained thumbnail photo attachments entitled "Exxxxx", "Mxxxxx," and "Gxxx."

FBI Found Malware on C.W.'s Laptop Computer that Would Allow a Remote Operator to Control Her Computer

14. On March 29, 2013, I participated in a forensic analysis of victim C.W.'s laptop computer. During the analysis, I learned the following:

a. The examination identified multiple executable files that appeared to be malware. This determination was made based upon the location of the files, registry entries causing the executable files to autorun, and strings within the executable files. The examining SA also found two files named "Blackshades," which appeared to be keylog files. Dates in the files indicated the malware generating the key log files was installed on or about June 7, 2012, and logging continued through the middle of March 2013. Online research into the name Blackshades indicated that Blackshades was malware that acted as a RAT. Searches of other strings found in the executable files indicated they may be associated with a RAT called DarkComet or NetWire. Details of the analysis of each potential malware sample revealed several times the malware connected to "cutefuzzypuppy.zapto.org" and "schedule2013.no-ip.org," connections which would be consistent with the operation of a RAT.

b. The words "Face", the first name of C.W., and C.W.'s Facebook password were found in the keylogging file on C.W.'s laptop. In his email messages, ABRAHAMS heckled C.W. for making her password so easy for him to guess on her Facebook account.

ABRAHAMS Identified as User of No-Ip.org and "Cutefuzzypuppy" Alias Found on C.W.'s Laptop Computer

15. Based on a nslookup done on March 29, 2013, and April 1, 2013, I learned that the domain name schedule2013@no-ip.org resolved to IP address 184.255.157.148 on both dates. A search was done to determine that the IP address belonged to Sprint.

16. I obtained and reviewed records from Sprint for the IP address 184.255.157.148. Based on those records, I learned that between March 29, 2013 and April 1, 2013, the IP address 184.255.157.148 was assigned to a Sprint customer named "EVERGREEN" with a billing address in Temecula, California. I further observed that the same IP address was assigned to the "EVERGREEN" account from March 20, 2013, through April 4, 2013.

17. I obtained and reviewed records from "No-ip.org" and learned the following:

a. The Domain name Schedule2013@no-ip.org had been configured to resolve to IP address 184.255.157.148 on March 21, 2013 at 19:00:45 PDT, the same date victim C.W. was first contacted by ABRAHAMS.

b. The Subscriber of the Schedule2013@no-ip.org account was in ABRAHAMS's father's name, with user name "cutefuzzypuppy", and email address johnshephard2@gmail.com.

c. In my interview of ABRAHAMS described later, ABRAHAMS told me that "John Shephard" was the name of a video game character.

18. I obtained and reviewed records obtained from Google pertaining to the email address johnshephard2@gmail.com and learned the following:

a. The subscriber was listed as John Shephard. The subscriber also listed a secondary email address that was a Yahoo! email address in ABRAHAMS's name;

b. The account used IP address 174.127.99.190, which is the Utah-based VPN used by ABRAHAMS;

c. The account used IP address 184.255.157.148, which is the IP used by the malware to call out to Schedule2013@no-ip.org on March 21, 2013;

d. Based on my training and experience, and work on this case, I came to the conclusion that ABRAHAMS was using Schedule2013@no-ip.org to disguise his involvement in the hacking of the victims' computers.

19. FBI analyst James Hassold conducted a search on the Internet for the name "cutefuzzypuppy" and told me the following:

a. On the website hackforums.net, a user named "cutefuzzypuppy" posted messages inquiring about, among other things, how to use VPNs and the malware Blackshades. The user named "cutefuzzypuppy" also showed interest in spreading malware through Tumblr and Facebook and in controlling webcams. In cutefuzzypuppy's postings on hackforums.net, the user bragged about infecting the computer of a person who "happen[ed] to be a model." C.W. is a model and beauty pageant winner. Portions of the messages from hackforums.net are described below:

i. April 11, 2012: "*I have recently purchased a FUD (fully undetectable) keylogger and I want to use it to hack*

a person's fb. However I suck at social engineering so what are some ways to get one to download and run a keylogger."

ii. May 17, 2012: "*Recently I infected a person at my school with darkcomet. It was total luck that I got her infected because I suck at social engineering. Anyway, this girl happens to be a model and a really..."*

iii. June 15, 2012, in response to a posting for Blackshades: "*Can I have a copy of this. It looks very good."*

iv. June 18, 2012, in response to a posting for "FREE VPN-USA,UK,GERMANY..": "*Hey! I need a good vpn. Could you please send me the link for this."*

v. June 26, 2012, in response to a posting for "How to hack a facebook account": "*Could you please pm this to me. Thanks in advance."*[4]

vi. July 12, 2012, in response to a posting for "Darkcomet slave limit?": "*I apologize in advance if this is a dumb question but I know that the amount of slaves you can have on a rat is limited to your internet connection speed. I am using Darkcomet and have a very slow..."*

vii. August 22, 2012: "*I am starting college on Monday and my college has a very fast internet connection. Normally at my house I have a very slow internet connection and that can make ratting difficult sometimes.."*

b. Additional online research on the username cutefuzzypuppy identified numerous posts on various gaming discussion boards. On one of these discussion boards, gamefaq.com, a user posting under the user ID Jabrahams276

---

[4] Based on my training and experience, I have seen "pm" used in Internet communications to be shorthand for "private message." Thus, I believed that ABRAHAMS was hoping to communicate directly and in a private forum with the user that posted the message with the subject "How to hack a facebook account" on hackforums.net.

identified his Xbox Live user ID as cutefuzzypuppy. Online research also identified a steam.com (a gaming-related website) account for user Cutefuzzypuppy. This user's profile used the first name of ABRAHAMS's brother and stated that the user lived in California.

Agents Learned More Information About ABRAHAMS

20. I performed a search on social media website Facebook and found out that ABRAHAMS was a college computer science student. Based on records obtained from his school, I learned that ABRAHAMS had used 174.127.99.190, the Utah-based VPN mentioned earlier that was used to send C.W. threatening emails, while on the school's network. School records showed that ABRAHAMS's school login used the IP address 184.255.157.148 -- the same IP address contacted by the RAT malware on C.W.'s computer -- on March 26, 2013, at 4:10 a.m., when the user logged onto the university's learning management system. School records showed that a user with ABRAHAMS's school login used the IP address 184.255.157.148 shortly after midnight on April 2, 2013, to take an online examination.

21. Based on records from Facebook, I learned that ABRAHAMS logged into his Facebook account from IP address 174.127.99.190.

22. FBI SA Michael Brown and I saw ABRAHAMS at his school. I recognized ABRAHAMS from his DMV photograph and a photograph taken while he was in high school.

ABRAHAMS Victimized E.L. in Maryland

23. A search of a multi-agency law enforcement database conducted by an FBI analyst determined that a complaint had been filed in Baltimore, Maryland on or about April 18, 2013, against

the F.L. aol.com email address taken over by ABRAHAMS for what appeared to be a similar extortion.

24. I contacted Baltimore County, Police Detective Derek Williams in Maryland, and learned the following:

a. Nineteen year-old victim E.L. reported that the target (later identified as ABRAHAMS) gained access to her Facebook and email accounts and then changed the passwords and photos;

b. ABRAHAMS contacted E.L. and sent a picture that looked like a partially nude photo of E.L., which was taken without her knowledge through her laptop webcam;

c. ABRAHAMS demanded more photographs or a Skype session with E.L. in exchange for his promise to delete the photos he had of her. ABRAHAMS threatened to upload the photographs of E.L. on her Facebook account, E.L.'s other accounts, and across the Web. ABRAHAMS also told E.L. that she could not tell anyone or he would upload E.L.'s pictures;

d. ABRAHAMS contacted E.L. using the F.L. aim.com email address and johnshephard22@gmail.com. ABRAHAMS had subscribed to Schedule2013@no-ip.org account using a similar Gmail email address, johnshephard2@gmail.com.

e. E.L.'s Yahoo! email address was one I recognized from having reviewed the pen register and trap and trace results for the two AOL email accounts that ABRAHAMS took over.

ABRAHAMS Victimized J.M. and J.M.'s Sister, M.M. #2, Using the P.S. Outlook.Com Email Address

25. On May 28, 2013, victim C.W. contacted me to say that she had received a message the previous day from ABRAHAMS using the P.S. Outlook.com email address. The message read, in part, as follows: "*Hey I ditched my old email address cuz I change*

emails every few months or so. But the real reason why I'm messaging you is because I have more facebook accounts (that all have mutual friends with you) then you could possibly imagine. I might message you directly on facebook but I haven't decided if I'm actually going to use your facebook or not. Anyway, block all the people, delete your account, whatever, just know that I finally decided I have enough facebooks and will upload your pictures on all of them. So yeah blah blah message me blah blah blah if not I'm posting your pictures ☺"

26. C.W. also told me she had received a Facebook message from J.M. In the email, J.M. said that she too had received an email from the P.S. Outlook.com email address. ABRAHAMS said in the email to J.M. that ABRAHAMS had thousands of nude pictures of J.M. and that ABRAHAMS had done the same thing to K.M. and M.L. ABRAHAMS blamed J.M. for allowing him to infect her friends' computers. ABRAHAMS threatened to upload the pictures if J.M. did not go on Skype with him. ABRAHAMS also threatened to upload the pictures if J.M. told anyone about this.

27. On May 29, 2013, I spoke with seventeen year-old J.M. who lives in Temecula, California, and she told me that she recognized herself in the pictures she had received from ABRAHAMS (who was now using the P.S. Outlook.com email address). J.M. said the pictures appeared as if they were taken via her webcam in her bedroom, at her aunt's house, and at her friend K.M.'s house.

28. On May 29, 2013, C.W. told me that she had received a Facebook message from J.M.'s Facebook account in which C.W. could see that someone had changed J.M.'s profile picture to a picture of C.W. In the message, ABRAHAMS told C.W. that he had placed a timer on C.W.'s computer. Thus, according to ABRAHAMS, when ten minutes had expired, her pictures would be uploaded and

shown to everyone unless C.W. messaged him (which would stop the timer). About an hour later, C.W. saw that a photograph showing her buttocks had been uploaded onto J.M.'s Facebook page.

29. On May 29, 2013, I spoke with the older, twenty-three year-old sister of J.M., M.M. #2, who told me she received an email from the P.S. Outlook.com email address which: said that ABRAHAMS had 1,000 photographs of her; said that ABRAHAMS had been stalking her since 2012; and instructed M.M. #2 to respond or Skype with ABRAHAMS. M.M. #2 told agents that M.M. #2 had also received an email from the P.S. Outlook.com email address which contained nude photographs of M.M. #2. She asked ABRAHAMS, "Why are you doing this to me?" and ABRAHAMS responded, "I told you I'll answer any questions after you Skype." M.M. #2 had been unaware that her younger sister, J.M., had also received emails from ABRAHAMS. M.M. #2 had used the same laptop computer as her younger sister and could tell the photographs were taken at her former address in approximately August 2012. M.M. #2 stopped responding to ABRAHAMS at the P.S. Outlook.com email address. While I spoke to M.M. #2 on the phone, she logged on to her Instagram account (a photo-sharing website) and found that nude photographs had been posted of her.

ABRAHAMS Victimized K.M. Using the P.S. Outlook.Com Email Address

30. On May 30, 2013, I spoke with sixteen year-old K.M. who lives in Temecula, California, who told me the following:

a. J.M. had contacted K.M. on May 27, 2013, and said J.M. had received an email from the P.S. Outlook.com email address that mentioned both K.M. and M.L. M.L. is a friend of the other victims and mentioned below;

b. J.M. warned K.M. about the P.S. Outlook.com email address because it was the same thing that happened to C.W.;

c. K.M. checked her Facebook account and determined that the password had been changed and she was locked out of it;

d. K.M. has also received emails from the P.S. Outlook.com email address but did not open them after receiving J.M.'s warning; however, K.M. could see that the messages began with the words "Kxxx(sic), Read This It's Important" and ""Proof These are not the Nudes I Will be Uploading".

ABRAHAMS Victimized M.L. Using the P.S. Outlook.Com Email Address

31. On May 30, 2013, I spoke with M.L. who lives in Temecula, California, and she told me the following:

a. J.M. had alerted M.L. to the threatening email messages that J.M. had received from the P.S. Outlook.com email address and the nude photographs J.M. had received;

b. M.L.'s email and Facebook accounts were hacked and messages were received from the P.S. Outlook.com email address, which M.L. did not open;

c. M.L. attempted to reset her passwords from her cousin's computer but her Facebook was hacked again.

ABRAHAMS Victimized Young Women Abroad as Well

32. An additional victim is M.M. #1. In an email to C.W., ABRAHAMS stated that M.M. #1 was an example of someone who immediately complied with his demands. The AOL pen register and trap and trace data included header information showing that ABRAHAMS communicated with M.M. #1's Hotmail email address. Based on online research, I believe that M.M. #1 lives in Ireland.

33. Based on my review of records from the F.L. aol.com email address and the P.S. Outlook.com email address, I have identified additional victims that I believe reside in foreign countries including Ireland, Canada, and Moldova.

Some Victims Complied with ABRAHAMS's Demands

34. Based on my review of records from the F.L. aol.com email address and the P.S. Outlook.com email address (including messages obtained from search warrants), I concluded that some victims did comply with ABRAHAMS's demands. For example, the email exchanges refer to the time and date when the victims agreed to go on Skype with ABRAHAMS. The messages also reveal the difficulty the victims had with the choices that ABRAHAMS gave them. Portions of the messages are as follows:

a. On April 11, 2013, M.M. #1 (who I believe lives in Ireland) wrote "I'm downloading Skype now. Please remember im only 17. Have a heart", to which ABRAHAMS responded "I'll tell you this right now! I do NOT have a heart!!! However I do stick to my deals! Also age doesn't mean a thing to me!!!"

b. On May 8, 2013, S.S. wrote "yesterday I requeted[sic] to not show my face is that okay", to which ABRAHAMS responded "You are going to be showing every part of you! I will not be recording or saving anything though."

Forensic Examiners Found Evidence of ABRAHAMS's Extortion and Hacking in Digital Devices Seized at His Residence

35. On June 4, 2013, federal search warrants were executed by agents of the FBI and detectives of the Temecula Police Department at ABRAHAMS's residence in Temecula, California. During the search, agents seized digital devices of ABRAHAMS, including a computer, a laptop, cell phone, and thumb drives.

36. The digital devices were later searched pursuant to the federal search warrants. Among other things, forensic examiners found evidence of hacking software and malware used to take over the victims' computers. The digital devices also had images and videos of some of the victims. In particular, based on my conversation with a forensic examiner, I learned that ABRAHAMS's cell phone appeared to contain images and videos of the victims organized by the victims' names. ABRAHAMS used an application on his cell phone that required a password to view the images and videos that appeared to be of the victims. One of the videos appeared to be a recording of a Skype session that ABRAHAMS had with one of his victims.

Statements Made by Jared ABRAHAMS on June 4, 2013

37. During the execution of search warrants at his residence, ABRAHAMS voluntarily agreed to speak with me and another agent. ABRAHAMS told me, among other things, the following:

a. ABRAHAMS is a college freshman. ABRAHAMS is studying computer science because he is good with computers;

b. C.W. is the first person (whose computer he hacked) that ABRAHAMS knew personally;

c. ABRAHAMS infected people's computers with the DarkComet malware so he could remotely operate their webcams, which he learned about on hacker forums;

d. ABRAHAMS was always at his computer so he would watch his victims change their clothes, and he would use the photographs against them;

e. ABRAHAMS contacted his victims using the email address of one of his non-important slave computers until the past week or two. Because he could no longer get into that email account, ABRAHAMS changed to the P.S. Outlook.com email address;

f. ABRAHAMS used the name "cutefuzzypuppy" because previously it had been used on gaming sites by his older brother;

g. ABRAHAMS succeeded in getting M.M. #1 to go on Skype and take her clothes off at his direction. After the Skype session, ABRAHAMS pretended to delete the original photos he had (of M.M. #1).

h. ABRAHAMS also succeeded in getting S.S. (of Canada) to undress and she was very upset about it.

i. ABRAHAMS obtained photographs via webcam of E.L. (of Baltimore, Maryland); G.B. (of Russia); J.M., K.M. and M.L. (of Temecula, California); and M.M. #2 (of Woodland Hills, California);

j. ABRAHAMS discussed creating an email account in the name of C.C. (a woman from Temecula, California) and sending emails to C.W. with that email account (acting as C.C.);

k. ABRAHAMS had about 30-40 slave computers at the time of the interview. ABRAHAMS had as many as 100-150 in the past when he was more actively involved in it (the hacking);

l. ABRAHAMS put the DarkComet malware on his desktop;

m. ABRAHAMS created two Domain Names, Schedule2013.no-ip.org and cutefuzzypuppy.zapto;

n. ABRAHAMS started using VPNs such as "NVPN" in Utah to stay anonymous and to stay safe;

o. ABRAHAMS focused on victim C.W. because she was well-known, but he knew it was wrong;

p. ABRAHAMS knew that some of the victims were under the age of eighteen;

q. ABRAHAMS acknowledged the aggression he used to coerce the victims to comply with his demands but said he is not normally aggressive.

VI.

CONCLUSION

38. Based upon the foregoing, I respectfully submit that there is probable cause to believe that ABRAHAMS committed extortion, in violation of Title 18, United States Code, Section 875(d).

/s/

Julie Patton, Special Agent
Federal Bureau of
Investigations

Subscribed to and sworn before me this 17th day of September, 2013.

ROBERT N. BLOCK

HONORABLE ROBERT N. BLOCK
UNITED STATES MAGISTRATE JUDGE